



(12) 发明专利申请

(10) 申请公布号 CN 112136302 A

(43) 申请公布日 2020.12.25

(21) 申请号 201980032528.8

(22) 申请日 2019.05.13

(30) 优先权数据

62/671,325 2018.05.14 US

(85) PCT国际申请进入国家阶段日

2020.11.13

(86) PCT国际申请的申请数据

PCT/US2019/031998 2019.05.13

(87) PCT国际申请的公布数据

WO2019/222090 EN 2019.11.21

(71) 申请人 维萨国际服务协会

地址 美国加利福尼亚州

(72) 发明人 O·威廉姆斯

(74) 专利代理机构 上海专利商标事务所有限公司 31100

代理人 徐倩 钱慰民

(51) Int.Cl.

H04L 29/06 (2006.01)

H04L 29/08 (2006.01)

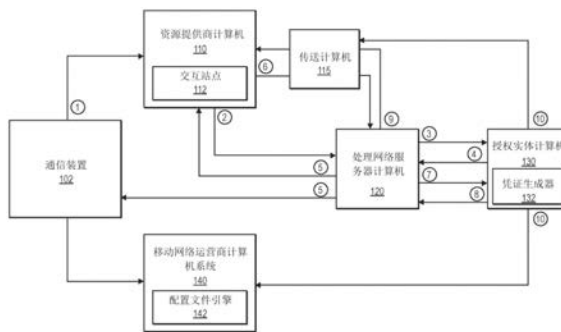
权利要求书3页 说明书13页 附图4页

(54) 发明名称

移动网络运营商认证协议

(57) 摘要

公开一种方法,且所述方法包括由服务器计算机接收对在资源提供商计算机与由用户操作且与移动网络运营商计算机系统相关联的通信装置之间进行的交互的虚拟访问凭证请求。所述方法还包括:由所述服务器计算机将所述虚拟访问凭证请求传输到授权实体计算机;由所述服务器计算机从所述授权实体计算机接收虚拟访问凭证;以及由所述服务器计算机将所述虚拟访问凭证传输到所述通信装置或所述资源提供商计算机。



1. 一种方法,包括:

由服务器计算机接收对在资源提供商计算机与由用户操作且与移动网络运营商计算机系统相关联的通信装置之间进行的交互的虚拟访问凭证请求;

由所述服务器计算机将所述虚拟访问凭证请求传输到授权实体计算机;

由所述服务器计算机从所述授权实体计算机接收虚拟访问凭证;

由所述服务器计算机将所述虚拟访问凭证传输到所述通信装置或所述资源提供商计算机;

由所述服务器计算机接收包括所述虚拟访问凭证的授权请求消息,其中所述授权请求消息请求对所述交互的授权;

由所述服务器计算机将所述授权请求消息转发到所述授权实体计算机;

由所述服务器计算机从所述授权实体计算机接收授权响应消息;以及

由所述服务器计算机将所述授权响应消息转发到所述资源提供商计算机,其中所述授权实体计算机随后完成与所述移动网络运营商计算机系统的交互。

2. 根据权利要求1所述的方法,其中所述虚拟访问凭证包括能用于访问位置或安全数据的数据。

3. 根据权利要求1所述的方法,其中所述通信装置是移动电话。

4. 根据权利要求1所述的方法,其中在由所述授权实体计算机确定所述虚拟访问凭证之前,所述移动网络运营商计算机系统执行与所述用户相关联的规则集合。

5. 根据权利要求1所述的方法,进一步包括:

生成与所述虚拟访问凭证相关联的用户配置文件;以及

将由所述授权实体计算机作出的确定与所述用户配置文件一起存储。

6. 一种计算机系统,包括:

处理器;以及

耦合到所述处理器的计算机可读介质,所述计算机可读介质包括能由所述处理器执行以用于实现方法的代码,所述方法包括:

接收对在资源提供商计算机与由用户操作且与移动网络运营商计算机系统相关联的通信装置之间进行的交互的虚拟访问凭证请求;

将所述虚拟访问凭证请求传输到授权实体计算机;

从所述授权实体计算机接收虚拟访问凭证;

将所述虚拟访问凭证传输到所述通信装置或所述资源提供商计算机;

接收包括所述虚拟访问凭证的授权请求消息,其中所述授权请求消息请求对所述交互的授权;

将所述授权请求消息转发到所述授权实体计算机;

从所述授权实体计算机接收授权响应消息;以及

将所述授权响应消息转发到所述资源提供商计算机,其中所述授权实体计算机随后完成与所述移动网络运营商计算机系统的交互。

7. 根据权利要求6所述的计算机系统,其中所述虚拟访问凭证的长度为16位数。

8. 根据权利要求6所述的计算机系统,其中所述移动网络运营商计算机系统将消息路由到多个无线模块装置以及从多个无线模块装置路由消息。

9. 根据权利要求6所述的计算机系统,其中在所述虚拟访问凭证被确定之前,所述移动网络运营商计算机系统执行与所述用户相关联的规则集合。

10. 根据权利要求6所述的计算机系统,进一步包括:

生成与所述虚拟访问凭证相关联的用户配置文件;以及

将由所述授权实体计算机作出的确定与所述用户配置文件一起存储。

11. 一种方法,包括:

由授权实体计算机接收对在资源提供商计算机与由用户操作且与移动网络运营商计算机系统相关联的通信装置之间进行的交互的虚拟访问凭证请求;

由所述授权实体计算机生成与已批准金额相关联的虚拟访问凭证;

由所述授权实体计算机将所述虚拟访问凭证传输到处理网络计算机,其中所述虚拟访问凭证被转发到所述通信装置或所述资源提供商计算机;

由所述授权实体计算机接收包括所述虚拟访问凭证的授权请求消息,其中所述授权请求消息请求对所述交互的授权;

将所述授权请求的总金额与所述虚拟访问凭证的所述已批准金额进行比较;

由所述授权实体计算机基于所述比较确定所述授权请求消息的批准或拒绝;

由所述授权实体计算机基于所述授权请求消息的所述批准或拒绝而生成授权响应消息;

由所述服务器计算机将所述授权响应消息转发到所述处理网络计算机;以及

随后基于所述授权请求消息的所述批准或拒绝将完成消息转发到所述移动网络运营商计算机系统。

12. 根据权利要求11所述的方法,其中所述虚拟访问凭证允许对安全数据的访问。

13. 根据权利要求11所述的方法,其中所述通信装置是移动电话。

14. 根据权利要求11所述的方法,其中在所述虚拟访问凭证被确定之前,所述移动网络运营商计算机系统执行与所述用户相关联的规则集合。

15. 根据权利要求11所述的方法,进一步包括:

生成与所述虚拟访问凭证相关联的用户配置文件;以及

将所述授权请求消息的所述批准或拒绝与所述用户配置文件一起存储。

16. 一种计算机系统,包括:

由授权实体计算机接收对在资源提供商计算机与由用户操作且与移动网络运营商计算机系统相关联的通信装置之间进行的交互的虚拟访问凭证请求;

由所述授权实体计算机生成与已批准金额相关联的虚拟访问凭证;

由所述授权实体计算机将所述虚拟访问凭证传输到处理网络计算机,其中所述虚拟访问凭证被转发到所述通信装置或所述资源提供商计算机;

由所述授权实体计算机接收包括所述虚拟访问凭证的授权请求消息,其中所述授权请求消息请求对所述交互的授权;

将所述授权请求的总金额与所述虚拟访问凭证的所述已批准金额进行比较;

由所述授权实体计算机基于所述比较确定所述授权请求消息的批准或拒绝;

由所述授权实体计算机基于所述授权请求消息的所述批准或拒绝而生成授权响应消息;

由所述服务器计算机将所述授权响应消息转发到所述处理网络计算机;以及
随后基于所述授权请求消息的所述批准或拒绝将完成消息转发到所述移动网络运营
商计算机系统。

17. 根据权利要求16所述的计算机系统,其中所述虚拟访问凭证允许对位置的访问。

18. 根据权利要求16所述的计算机系统,其中所述通信装置是笔记本电脑。

19. 根据权利要求16所述的计算机系统,其中在所述虚拟访问凭证被确定之前,所述移
动网络运营商计算机系统执行与所述用户相关联的规则集合。

20. 根据权利要求16所述的计算机系统,进一步包括:

生成与所述虚拟访问凭证相关联的用户配置文件;以及

将所述授权请求消息的所述批准或拒绝与所述用户配置文件一起存储。

移动网络运营商认证协议

[0001] 相关申请交叉引用

[0002] 本申请要求2018年5月14日提交的第62/671,325号美国临时申请的权益,所述美国临时申请出于所有目的以全文引用的方式并入本文中。

背景技术

[0003] 存在用户可能不会拥有适当的凭证但可能希望能够访问资源的许多情况。在一个示例中,人们可能希望进入建筑物,但可能没有建筑物门禁的适当身份卡或钥匙卡。在另一个示例中,人们可能希望购买物品,但可能没有电子借记卡或信用卡来购买该物品。希望在用户没有访问凭证的情况下为用户提供对资源的访问。

[0004] 本发明的实施例单独和共同地解决了上述问题和其它问题。

发明内容

[0005] 本公开的实施例涉及提供对访问的认证和授权的方法和系统。在一些示例中,所述方法和系统将建立第一和第二级认证,其中授权实体可以建立第一认证且移动网络运营商计算机可以建立第二认证。在其它示例中,系统将允许用户使用与用户的通信装置相关联的移动网络运营商计算机系统而不是银行的账户来发起购买交易或访问受限区域。

[0006] 本发明的一个实施例涉及一种方法或系统,包括:由服务器计算机接收对在资源提供商计算机与由用户操作且与移动网络运营商计算机系统相关联的通信装置之间进行的交互的虚拟访问凭证请求;由所述服务器计算机将所述虚拟访问凭证请求传输到授权实体计算机;由所述服务器计算机从所述授权实体计算机接收虚拟访问凭证;由所述服务器计算机将所述虚拟访问凭证传输到所述通信装置或所述资源提供商计算机;由所述服务器计算机接收包括所述虚拟访问凭证的授权请求消息,其中所述授权请求消息请求对所述交互的授权;由所述服务器计算机将所述授权请求消息转发到所述授权实体计算机;由所述服务器计算机从所述授权实体计算机接收授权响应消息;以及由所述服务器计算机将所述授权响应消息转发到所述资源提供商计算机,其中所述授权实体计算机随后完成与所述移动网络运营商计算机系统的所述交互。

[0007] 本发明的另一实施例涉及:由授权实体计算机接收对在资源提供商计算机与由用户操作且与移动网络运营商计算机系统相关联的通信装置之间进行的交互的虚拟访问凭证请求;由所述授权实体计算机生成与已批准金额相关联的虚拟访问凭证;由所述授权实体计算机将所述虚拟访问凭证传输到处理网络计算机,其中所述虚拟访问凭证被转发到所述通信装置或所述资源提供商计算机;由所述授权实体计算机接收包括所述虚拟访问凭证的授权请求消息,其中所述授权请求消息请求对所述交互的授权;将所述授权请求的总金额与所述虚拟访问凭证的所述已批准金额进行比较;由所述授权实体计算机基于所述比较确定所述授权请求消息的批准或拒绝;由所述授权实体计算机基于所述授权请求消息的所述批准或拒绝而生成授权响应消息;由所述服务器计算机将所述授权响应消息转发到所述处理网络计算机;以及随后基于所述授权请求消息的所述批准或拒绝将完成消息转发到所

述移动网络运营商计算机系统。

[0008] 其它实施例涉及适于执行上述方法和其它方法的服务器计算机和系统。

[0009] 下文进一步详细描述本发明的这些和其它实施例。

附图说明

[0010] 图1示出根据本发明的实施例的认证和授权系统的框图。

[0011] 图2示出根据本发明的实施例的处理网络服务器计算机的框图。

[0012] 图3示出根据本发明的实施例的资源提供商计算机的框图。

[0013] 图4示出根据本发明的实施例的授权实体计算机的框图。

[0014] 图5示出根据本发明的实施例的移动网络运营商计算机系统的框图。

[0015] 图6示出根据本发明的实施例的通信装置的框图。

具体实施方式

[0016] 在论述本发明的实施例之前,对一些术语的进一步描述可能有助于理解本发明的实施例。

[0017] “虚拟访问凭证”可以是具有有限使用寿命或有限使用次数的凭证。如下文进一步描述,虚拟访问凭证可以具有凭证或支付凭证、令牌或支付令牌的形式或属性。虚拟访问凭证可用于获得例如商品、服务、位置和安全数据等资源。虚拟访问凭证还可以有任何合适的形式,包括字母或数字(例如,16位数的数字)。

[0018] “凭证”可以是充当价值、所有权、身份或权限的可靠证据的任何合适的信息。凭证可以是一串数字、字母或任何其它合适的字符,以及可用作确认的任何对象或文件。凭证的示例包括价值凭证,例如支付凭证、标识卡、认证文件、通行卡、密码和其它登录信息等。

[0019] “支付凭证”可包括与账户相关联的任何合适信息(例如,与账户相关联的支付账户和/或支付装置)。此类信息可以与账户直接相关,或可以源自与账户相关的信息。账户信息的示例可包括PAN(主账号或“账号”)、用户名、有效期以及验证值,例如CVV、dCVV、CVV2、dCVV2和CVC3值。

[0020] “数字钱包”可以包括允许个人进行电子商务交易的电子装置。电子钱包可存储用户配置文件信息、支付凭证、银行账户信息、一个或多个数字钱包标识符等,并且可以用在各种交易中,例如但不限于电子商务、社交网络、转账/个人支付、移动商务、近距离支付、游戏等,以用于零售购买、数字商品购买、公用事业支付、从游戏网站购买游戏或游戏点券、用户之间转移资金等。数字钱包可以被设计来简化购买和支付过程。数字钱包可以允许用户将一个或多个支付卡加载到数字钱包上,以便进行支付而无需输入账号或出示实体卡。

[0021] “令牌”可以是凭证的取代值。令牌可以是一串数字、字母或任何其它合适的字符。令牌的示例包括支付令牌、访问令牌、个人标识令牌等。

[0022] “支付令牌”可以包括支付账户的标识符,它是账户标识符的取代,例如主账号(PAN)。例如,支付令牌可包括可用作原始账户标识符的取代的一系列字母数字字符。例如,令牌“4900 0000 0000 0001”可用于代替PAN“4147 0900 0000 1234”。在一些实施例中,支付令牌可以是“保留格式的”,并且可具有与现有交易处理网络中使用的账户标识符一致的数值格式(例如,ISO 8583金融交易消息格式)。在一些实施例中,支付令牌可代替PAN用来

发起、授权、结算或解决支付交易,或在通常会提供原始凭证的其它系统中表示原始凭证。在一些实施例中,可生成支付令牌,使得可能无法以计算方式从令牌值得出原始PAN或其它账户标识符的恢复。此外,在一些实施例中,令牌格式可被配置成允许接收令牌的实体将其标识为令牌并辨识发行令牌的实体。

[0023] “令牌化”是用取代数据替换数据的过程。例如,可通过利用可与支付账户标识符相关联的取代编号(例如,令牌)替换主账户标识符来将支付账户标识符(例如,主账号(PAN))令牌化。此外,令牌化可应用于可用取代值(即,令牌)替换的任何其它信息。令牌化提高交易效率和安全性。

[0024] “虚拟访问凭证请求消息”可以是请求虚拟访问凭证的电子消息。虚拟访问凭证请求消息可以包括可用于标识支付账户或数字钱包的信息,和/或用于生成虚拟访问凭证的信息。例如,虚拟访问凭证请求消息可以包括支付凭证、移动装置标识信息(例如,电话号码或MSISDN)、数字钱包标识符、标识令牌化服务提供商的信息、商家标识符、密码和/或任何其它合适的信息。虚拟访问凭证请求消息中包括的信息可以(例如,使用授权实体特定的密钥)进行加密。在一些示例中,虚拟访问凭证请求消息可以包括代表授权实体计算机向用户提供的已批准金额(例如,借记金额等),并且所述已批准金额存储在授权实体计算机处的用户配置文件中以在稍后的时间与授权请求消息中包括的总金额进行比较。

[0025] “虚拟访问凭证响应消息”可以是响应虚拟访问凭证请求的消息。虚拟访问凭证响应消息可以包括虚拟访问凭证请求被批准或拒绝的指示。虚拟访问凭证响应消息还可以包括虚拟访问凭证、移动装置标识信息(例如,电话号码或MSISDN)、数字钱包标识符、标识令牌化服务提供商的信息、资源提供商标识符、密码和/或任何其它合适的信息。虚拟访问凭证响应消息中包括的信息可以(例如,使用发行方特定的密钥)进行加密。

[0026] “用户”可以包括个人。在一些实施例中,用户可以与一个或多个个人账户和/或移动装置相关联。在一些实施例中,用户也可被称为持卡人、账户持有人或消费者。

[0027] “授权请求消息”可以是请求对交易的授权的电子消息。在一些实施例中,授权请求消息被发送给交易处理计算机和/或支付卡的发行方,以请求交易授权。根据一些实施例的授权请求消息可符合ISO8583,这是针对交换与用户使用支付装置或支付账户进行的支付相关联的电子交易信息的系统的标准。授权请求消息可以包括可以与支付装置或支付账户相关联的发行方账户标识符。授权请求消息还可以包括与“标识信息”相对应的额外数据元素,包括(只作为示例):服务代码、CVV(卡验证值)、dCVV(动态卡验证值)、PAN(主账号或“账号”)、支付令牌、用户名、有效期等。授权请求消息还可以包括“交易信息”,例如与当前交易相关联的任何信息,例如交易总金额、商家标识符、商家位置、收单方银行标识号(BIN)、卡片接受器ID、标识正购买的物品的信息等,以及可用于确定是否标识和/或授权交易的任何其它信息。

[0028] “授权响应消息”可以是响应于授权请求的消息。在一些情况下,授权响应消息可以是由发行金融机构或交易处理计算机生成的对授权请求消息的电子消息应答。仅借助于示例,授权响应消息可以包括以下状态指示符中的一个或多个:批准-交易被批准;拒绝-交易未被批准;或呼叫中心-响应未决的更多信息,商家必须呼叫免费授权电话号码。授权响应消息还可包括授权代码,所述授权代码可以是信用卡发行银行响应于电子消息中的授权请求消息(直接地或通过交易处理计算机)返回到商家的访问装置(例如,POS设备)的指示

交易被批准的代码。所述代码可充当授权的证明。

[0029] “服务器计算机”可以包括功能强大的计算机或计算机集群。例如，服务器计算机可以是大型主机、小型计算机集群或作为一个单元起作用的一组服务器。在一个示例中，服务器计算机可以是耦合到网络服务器的数据库服务器。服务器计算机可包括一个或多个计算设备，并且可使用多种计算结构、布置和编译中的任一种来服务来自一个或多个客户端计算机的请求。

[0030] 本公开的实施例包括提供对访问的认证和授权的方法和系统。在一些示例中，系统将建立第一和第二级认证，其中授权实体可以建立第一认证且移动网络运营商计算机可以建立第二认证。在其它示例中，系统将允许用户使用与用户的通信装置相关联的移动网络运营商计算机系统而不是银行的账户来发起购买交易或访问受限区域。

[0031] 图1示出根据本发明的实施例的认证和授权系统的框图。如图所示，系统可以包括通信装置102、资源提供商计算机110、传送计算机115、处理网络服务器计算机120、授权实体计算机130以及移动网络运营商计算机系统140。

[0032] 图1的系统可以包括处理网络服务器计算机120。图1的示例处理网络服务器计算机120如图2所示。处理网络服务器计算机120可以包括一个或多个服务器计算机，以及数据处理子系统、网络和支持和传递授权服务、异常文件服务以及清算和结算服务的操作。示例性处理网络可以包括VisaNet™。例如VisaNet™的处理网络能够处理信用卡交易、借记卡交易以及其它类型的商业交易。VisaNet™确切地说包括处理授权请求的VIP系统(Visa集成式支付系统)，和执行清算和结算服务的Base II系统。处理网络可以使用包括因特网的任何合适的有线或无线网络。

[0033] 处理网络服务器计算机可以包括如图2所示的经由系统总线210互连的子系统或部件。经由系统总线210的互连允许处理器212与每个子系统通信，并控制来自系统存储器214的指令的执行。系统存储器214可以体现计算机可读介质。通信接口216可以用于将服务器计算机连接到例如因特网的广域网或与计算机系统相关联的其它I/O装置。系统总线210还可以连接在存储器中体现的一个或多个模块或引擎，包括通信模块230、虚拟访问凭证模块232和/或交互引擎234。

[0034] 通信模块230可以被配置成在图1中所示的整个系统中接收和传输来自其它计算机和装置的消息。例如，通信模块230可以被配置成接收来自通信装置102的虚拟访问凭证请求、将虚拟访问凭证请求传输到授权实体计算机130、接收和传输虚拟访问凭证、接收和传输授权请求消息，以及接收和传输授权响应消息。

[0035] 虚拟访问凭证模块232可以被配置成解析虚拟访问凭证请求，以确定与由用户操作的通信装置102相关联的用户标识符。用户标识符可以与移动网络运营商计算机系统140相对应，以接收与用户标识符相关联的附加信息。附加信息可以包括在移动网络运营商计算机系统140注册的通信装置的订单历史记录、位置历史记录或用户配置文件信息。虚拟访问凭证模块232可以确定是否基于附加信息生成虚拟访问凭证。

[0036] 交互引擎234可以被配置成基于虚拟访问凭证来标识授权实体计算机130，并且将授权请求消息路由到适当的授权实体计算机130。例如，授权请求消息可以包括凭证，凭证包括唯一地标识多个授权实体计算机中的一个授权实体计算机的银行标识号(BIN)。交互引擎234可以将接收的BIN与合适的路由信息关联到授权实体计算机，并且使得能够将授权

请求消息传输到适当的授权实体计算机。

[0037] 图1的系统还可以包括资源提供商计算机110。图1的示例资源提供商计算机110如图3所示。资源提供商计算机可以是可以提供例如商品、服务、信息和/或访问等资源的实体。资源提供商的示例包括商家、数据提供商、运输代理、政府实体、场地和住宅运营商等。商家通常可为参与交易且能够出售商品或服务或提供对商品或服务的访问的实体。

[0038] 资源提供商计算机可以包括如图3所示的经由系统总线310互连的子系统或部件。经由系统总线310的互连允许处理器312与每个子系统通信,并控制来自系统存储器314的指令的执行。系统存储器314可以体现计算机可读介质。通信接口316可以用于将资源提供商计算机连接到例如因特网的广域网或与资源提供商计算机相关联的其它I/O装置。系统总线310还可以连接在存储器中体现的一个或多个模块或引擎,包括通信模块330、请求引擎332和/或交互引擎334。一个或多个数据库可以存储由资源提供商计算机接收、维护和传输的信息,包括物品数据库350。

[0039] 通信模块330可以被配置成在图1中所示的整个系统中接收和传输来自其它计算机和装置的消息。例如,通信模块可以被配置成接收对订购交互站点112处的物品或服务的请求、接收交互站点112处的交互的指示(例如,选择“给我开具账单(bill me)”按钮等)、将虚拟访问凭证请求传输到处理网络服务器计算机120,以及将授权请求消息传输到传送计算机115。

[0040] 请求引擎332可以被配置成生成与通信装置102与交互站点112(图3中未示出)之间的交互相关联的虚拟访问凭证请求。虚拟访问凭证请求可以包括与由用户操作的通信装置相关联的信息。在一些实施例中,虚拟访问凭证可以对应于与对访问通信装置102请求的资源的请求相关联的已批准金额。金额可以由授权实体计算机130批准。

[0041] 请求引擎332还可以被配置成生成授权请求消息,其包括从授权实体计算机130接收的虚拟访问凭证和与通信装置102请求的资源相关联的总金额。请求引擎332可以将授权请求消息与资源提供商计算机110提供的一个或多个资源(例如,物品或服务)相关联。资源可以对应于物品数据库350中存储的物品描述、价值金额以及其它相关信息。

[0042] 交互引擎334可以被配置成在认证虚拟访问凭证以及与包括来自授权实体计算机130的批准确定的授权响应消息相关联的授权后允许访问资源。

[0043] 资源提供商计算机110还可以与访问装置相关联。访问装置可以由资源提供商操作,并且可以包括提供对远程系统的访问的任何合适的装置。访问装置还可以用于与资源提供商计算机110、交易处理计算机、认证计算机或任何其它合适的系统通信。访问装置一般可以位于任何合适的位置,例如,位于资源提供商的位置。访问装置可以采用任何合适的形式。访问装置的一些示例包括POS或销售点装置(例如,POS终端)、蜂窝电话、PDA、个人计算机(PC)、平板PC、手持式专用读取器、机顶盒、电子现金出纳机(ECR)、自动柜员机(ATM)、虚拟现金出纳机(VCR)、查询一体机、安全系统、访问系统等。访问装置可以使用任何合适的接触或非接触操作模式,以发送或接收来自移动通信装置或者支付装置的数据或与移动通信装置或者支付装置相关联的数据。在访问装置可包括POS终端的一些实施例中,可使用任何合适的POS终端且其可包括读取器、处理器和计算机可读介质。读取器可以包括任何合适的接触或非接触操作模式。例如,示例性读卡器可以包括射频(RF)天线、光学扫描器、条形码读取器或磁条读取器,以与支付装置和/或移动装置交互。在一些实施例中,用作POS终端

的蜂窝电话、平板电脑或其它专用无线装置可被称为移动销售点或“mPOS”终端。

[0044] 图1的系统还可以包括传送计算机115。传送计算机115可以由收单方或与特定商家或其它实体具有业务关系的业务实体(例如,商业银行)操作。一些实体可以执行发行方功能和收单方功能两者。一些实施例可以涵盖此类单个实体发行方-收单方。

[0045] 图1的系统还可以包括授权实体计算机130。示例授权实体计算机130如图4所示。授权实体可以是授权请求的实体。授权实体的示例可以是发行方、政府机构、文件存储库、访问管理员、银行等。授权实体计算机130通常可以指维护用户账户的业务实体(例如,银行或发行方计算机)。

[0046] 授权实体计算机可以包括如图4所示的经由系统总线410互连的子系统或部件。经由系统总线410的互连允许处理器412与每个子系统通信,并控制来自系统存储器414的指令的执行。系统存储器414可以体现计算机可读介质。通信接口416可以用于将授权实体计算机连接到例如因特网的广域网或与授权实体计算机相关联的其它I/O装置。系统总线410还可以连接在存储器中体现的一个或多个模块或引擎,包括通信模块430、虚拟访问凭证模块432和/或授权模块434。一个或多个数据库可以存储由授权实体计算机接收、维护和传输的信息,包括凭证数据库450。

[0047] 通信模块430可以被配置成在图1中所示的整个系统中接收和传输来自其它计算机和装置的消息。例如,通信模块430可以被配置成从处理网络服务器计算机120接收虚拟访问凭证请求、将虚拟访问凭证传输到处理网络服务器计算机120、接收授权请求消息、生成并传输授权响应消息,并且在通信装置102与资源提供商计算机110之间已经发生交互之后传输与清算和结算相关联的消息。

[0048] 虚拟访问凭证模块432可以被配置成生成虚拟访问凭证并将虚拟访问凭证发给通信装置102,例如蜂窝电话、智能卡、平板电脑或笔记本电脑。虚拟访问凭证可以包括与由用户操作的通信装置相关联的用户标识符。用户标识符可以与在移动网络运营商计算机系统140注册的用户账户相对应。虚拟访问凭证还可以与订购资源提供商计算机110提供的资源的已批准金额相对应。

[0049] 授权模块434可以被配置成至少部分地基于将响应于虚拟访问凭证请求而提供的第一虚拟访问凭证与随授权请求消息接收的第二虚拟访问凭证进行比较来确定是允许还是拒绝对资源提供商计算机110提供的资源的访问。虚拟访问凭证可以存储在凭证数据库450中并且与通信装置102或用户相关联。

[0050] 授权模块434还可以被配置成至少部分地基于将包括在授权请求消息中的总金额与代表授权实体计算机向用户提供的已批准金额进行比较来确定是允许还是拒绝对资源提供商计算机110提供的资源的访问。已批准金额可以存储在授权实体计算机130处的用户配置文件和虚拟访问凭证中。

[0051] 图1的系统还可以包括移动网络运营商计算机系统140。示例移动网络运营商计算机系统140如图5所示。移动网络运营商计算机系统140可以包括为移动装置(包括通信装置102)提供移动网络服务的实体。移动网络运营商计算机系统140可以执行无线电频谱分配、无线网络基础架构等。移动网络运营商计算机系统140可以通过与移动装置的一个或多个对应用户相关联的用户账户标识移动装置。移动网络运营商计算机系统140还可以向用户提供发票或账单,以换取提供移动网络服务。

[0052] 移动网络运营商计算机系统可以包括如图5所示的经由系统总线510互连的子系统或部件。经由系统总线410的互连允许处理器512与每个子系统通信,并控制来自系统存储器514的指令的执行。系统存储器514可以体现计算机可读介质。通信接口516可以用于将资源提供商计算机连接到例如因特网的广域网或与资源提供商计算机相关联的其它I/O装置。系统总线510还可以连接在存储器中体现的一个或多个模块或引擎,包括通信模块530、交互引擎532和/或网络操作引擎534。一个或多个数据库可以存储由移动网络运营商计算机系统(包括用户数据库550)接收、维护和传输的信息。

[0053] 通信模块530可以被配置成在图1中所示的整个系统中接收和传输来自其它计算机和装置的消息。例如,通信模块530可以被配置成向通信装置102提供移动网络服务、从通信装置102接收包括支付提供移动网络服务的发票的通信,并接收和传输与授权实体计算机130的通信,包括与结算和清算过程相关联的消息。

[0054] 交互引擎532可以被配置成通过提供移动网络通信服务的过程来确定与通信装置102相关联的订单历史记录、位置历史记录或用户配置文件信息。例如,用户可以从移动网络运营商计算机系统140定期订购移动网络通信服务。订购服务的历史记录可以由配置文件引擎142接收和处理,并且存储在用户数据库550中。在一些示例中,通信装置102可以传输位置消息,所述位置消息由移动网络运营商计算机系统140接收并存储在用户数据库550中,以生成与通信装置102相关联的位置信息的历史记录。

[0055] 网络操作引擎534可以被配置成执行无线电频谱分配、无线网络基础架构等。网络操作引擎534可以通过与装置的一个或多个对应用户相关联的用户账户标识通信装置102。

[0056] 图1的系统可以包括通信装置120。图1的示例通信装置102如图6所示。通信装置可以包括可由用户操作的任何合适的电子装置,所述电子装置还可提供与网络的远程通信功能。移动通信装置可以是可容易传送的通信装置的示例。远程通信功能的示例包括使用移动电话(无线)网络、无线数据网络(例如,3G、4G或类似网络)、Wi-Fi、Wi-Max,或可以提供对例如因特网或专用网络的网络的访问的任何其它通信介质。移动通信装置的示例包括移动电话(例如,蜂窝电话)、PDA、平板电脑、上网本、笔记本电脑、个人音乐播放器、手持式专用读取器等。移动通信装置的其它示例包括可穿戴式装置,例如智能手表、健身手环、脚链、戒指、耳环等,以及具有远程通信功能的汽车。在一些实施例中,移动通信装置可以充当支付装置(例如,移动通信装置可以存储并且能够传输用于交易的支付凭证)。

[0057] 支付装置可以并入有通信装置102并且包括可以用于进行金融交易以向商家提供支付凭证的任何合适的装置。支付装置可以是软件对象(例如,与信用、借记或预付账户相关联的支付应用程序)、硬件对象或物理对象。支付装置可以与例如货币价值、折扣或商店信用的值相关联,并且支付装置可以与例如银行、商家、支付处理网络或个人的实体相关联。

[0058] 图6的通信装置600可以包括处理器602和主体614。其还可以包括计算机可读介质604。计算机可读介质604可以呈存储交易数据的存储器的形式(或可以包括所述存储器在中),并且可以呈包括磁条、存储器芯片等的任何合适的形式。存储器可以存储例如财务信息的信息,包括银行账户信息、账户余额信息、有效期,或消费者信息,例如账户持有人的姓名、出生日期等。这些信息中的任何信息可以由通信装置600经由天线618传输。

[0059] 通信装置600可以进一步包括非接触元件612,所述非接触元件可以半导体芯片或

具有例如天线618的相关无线传递(例如,数据传输)元件的其它数据存储元件的形式实现。非接触元件612可以与通信装置600相关联或嵌入于所述通信装置内。数据或控制指令可以经由蜂窝网络传输,并且可以借助于非接触元件接口(未示出)而应用于非接触元件612。非接触元件接口可用以允许在装置电路系统(以及因此蜂窝网络)与任选的非接触元件之间交换数据和/或控制指令。

[0060] 非接触元件612可能使用根据标准化协议或数据传递机构(例如,ISO14443/NFC)的近场通信(NFC)来传递和接收数据。近场通信功能可以包括短程通信功能,包括RFID、蓝牙、红外线,或可以用于在通信装置与询问装置之间交换数据的其它数据传递功能。因此,通信装置可能通过近场通信经由蜂窝网络传送和传递数据和/或控制指令。

[0061] 通信装置还可包括用于处理通信装置的功能的处理器602。通信装置还可包括允许用户经由用户界面看见信息和消息的显示器606。通信装置可以进一步包括允许用户向通信装置提供信息的输入元件608、允许用户进行安全语音通信、音乐等的扬声器610。通信装置还可包括允许用户通过通信装置传输其语音或其它声音文件的麦克风616。通信装置还可包括用于无线数据传递和传输的天线618。

[0062] 返回到图1的步骤1,由用户操作的通信装置102可以与资源提供商计算机110交互。资源提供商计算机110可以提供交互站点112以接收来自通信装置102的一个或多个交互。在一些示例中,资源提供商计算机110可以提供可以存储在通信装置102中并由通信装置102执行的应用程序。通信装置102可以在通信装置102的显示器处呈现应用程序以接收来自通信装置102处的用户的交互。

[0063] 交互站点112(或应用程序)可以提供用于订购的一个或多个物品或服务。通信装置102可以与一个或多个物品或服务交互,将物品添加到资源提供商计算机110的交互站点112附带的电子购物车。交互站点112(或应用程序)也可以提供“给我开具账单”按钮。“给我开具账单”按钮在被选择时可以与处理网络服务器计算机120发起对电子购物车内包括的物品的交易。

[0064] 资源提供商计算机110可以通过交互站点112处提供的“给我开具账单”按钮接收来自通信装置102的交互。例如,在用户选择要添加到资源提供商计算机110上的电子购物车的物品之后,用户可以选择所述按钮来发起订购物品。交互可以与添加到电子购物车的物品的总价值相关联。

[0065] 在一些示例中,用户可能没有预先存在的信用或借记账户,或者不可使用预先存在的信用或借记账户进行此特定购买。在这些示例中,与通信装置102相关联的用户可能没有授权实体计算机的用户账户。因此,在交互站点112提供了“给我开具账单”按钮并且此按钮被选择时,用户可能不与信用或借记账户对应以完成物品或服务的购买。

[0066] 在步骤2,一旦经由通信装置102选择了“给我开具账单”按钮,便将(经由交互站点112或通信装置102处存储的应用程序)从资源提供商计算机110发送虚拟访问凭证请求到处理网络服务器计算机120。在一些示例中,虚拟访问凭证请求可以标识与通信装置102相对应的用户,以支持对交互授权的请求(例如,在激活了“给我开具账单”按钮时完成电子购物车中的物品或服务的交易,等等)。在一些示例中,添加到电子购物车的物品的总价值可以包括在虚拟访问凭证请求中。

[0067] 在接收到请求时,处理网络服务器计算机120可以发起虚拟访问凭证的生成。在交

易之前,虚拟访问凭证可不与用户的预先存在账户绑定。在一些情况下,用户可被视为“无银行账户的”,并且可能没有任何银行的任何类型的银行账户,但可能具有移动网络运营商计算机系统140的账户。

[0068] 在步骤3,处理网络服务器计算机120可以与授权实体计算机130通信,所述授权实体计算机然后可以生成虚拟访问凭证。虚拟访问凭证可以与与操作通信装置102的用户相关联的移动网络运营商计算机系统140相关联而不与用户本身相关联。例如,授权实体计算机130可以将企业信贷扩展到移动网络运营商计算机系统140而非用户。移动网络运营商计算机系统140可以是代替用户进行交易的一方。

[0069] 在生成虚拟访问凭证之前,授权实体计算机130可以执行与用户相关联的规则集合,以确定是否可以将虚拟访问凭证发行到移动网络运营商计算机系统140。例如,授权实体计算机130可以确定移动网络运营商计算机系统140是否提供了“选择加入”通信,以为其用户提供信用。在一些示例中,“选择退出”通信可以标识移动网络运营商计算机系统140将不支持为其用户发行虚拟访问凭证。

[0070] 移动网络运营商计算机系统140也可以执行与用户相关联的规则集合,以确定是否可以将虚拟访问凭证发行给操作与移动网络运营商计算机系统140相关联的通信装置的用户。移动网络运营商计算机系统140可以标识合适的信息,例如通信装置102的装置信息、移动网络运营商计算机系统140或资源提供商计算机110可能具有的关于用户的任何数据、历史订单或支付信息等。

[0071] 在一些示例中,移动网络运营商计算机系统140可以执行与用户相关联的规则集合,以确定是否可以发行虚拟访问凭证。授权实体计算机130可以与移动网络运营商计算机系统140相对应,以接收移动网络运营商计算机系统140的关于是否基于执行与用户相关联的规则集合而向用户发行虚拟访问凭证的确定。基于移动网络运营商计算机系统140的确定,授权实体计算机130可以生成虚拟访问凭证。

[0072] 虚拟访问凭证可以包括可重复使用或一次性使用的账户标识符。当虚拟访问凭证可重复使用时,凭证可以存储在移动网络运营商计算机系统140处的用户配置文件中且与其相关联,并且用于超过一次交易。当虚拟访问凭证是一次性使用的账户标识符时,可以针对每个潜在交易在资源提供商计算机110与处理网络服务器计算机120之间传输虚拟访问凭证请求。在任一示例中,虚拟访问凭证可以存储在授权实体计算机130的凭证数据库450中,以在授权过程期间检索和使用。在一些示例中,虚拟访问凭证可以与用户账户一起存储于授权实体计算机130处。用户账户可以包括通过虚拟访问凭证请求的总价值。

[0073] 在步骤4,授权实体计算机130可以向处理网络服务器计算机120提供虚拟访问凭证。处理网络服务器计算机120可以从授权实体计算机130获得虚拟访问凭证。

[0074] 在步骤5,处理网络服务器计算机120可以将虚拟访问凭证从授权实体计算机130传输到资源提供商计算机110或通信装置102以进行处理。经其移动应用程序或交互站点112,资源提供商计算机110可以使用虚拟访问凭证处理交易。例如,资源提供商计算机110可以生成包括虚拟访问凭证的授权请求消息。资源提供商计算机110可以在授权请求消息中包括虚拟访问凭证,以发起与“给我开具账单”按钮相关联且位于电子购物车中的物品和服务的交易。

[0075] 在一些示例中,“给我开具账单”按钮位于通信装置102处存储的应用程序处。可以

将虚拟访问凭证提供给通信装置102的应用程序,并且应用程序可以生成包括源自通信装置102处的应用程序的虚拟访问凭证的授权请求消息。可以将授权请求消息从通信装置102传输到资源提供商计算机110。

[0076] 在步骤6,资源提供商计算机110可以将包括虚拟访问凭证的授权请求消息传输到传送计算机115。传送计算机115可以将授权请求消息传输到处理网络服务器计算机120。处理网络服务器计算机120可以接收包括虚拟访问凭证的授权请求消息,其中授权请求消息请求对交互的授权。

[0077] 在一些示例中,处理网络服务器计算机120可以基于解析虚拟访问凭证来标识授权实体计算机130。例如,虚拟访问凭证可以包括唯一地标识处理网络服务器计算机120的授权实体的子字符串。子字符串可以类似于存储在处理网络服务器计算机120中的银行标识号(BIN)。当虚拟访问凭证的子字符串与存储的信息匹配时,处理网络服务器计算机120可以标识适当授权实体的位置以传输授权请求消息。

[0078] 在步骤7,处理网络服务器计算机120可以将授权请求消息转发到授权实体计算机130。授权实体计算机130可以确定是批准还是拒绝交易。例如,在批准或拒绝过程期间,授权实体计算机130可以将授权请求消息中包括的交易价值与虚拟访问凭证中包括的且存储于用户账户的总价值进行比较。当交易价值在总价值的阈值范围内时,交易可被批准。否则,由于交易的授权请求消息中包括的交易价值与虚拟访问凭证请求中包括的总价值不匹配,因此交易可能被拒绝。

[0079] 在步骤8,授权实体计算机130可以向处理网络服务器计算机120生成包括批准或拒绝交易的授权响应消息。处理网络服务器计算机120可以从授权实体计算机130接收授权响应消息。

[0080] 在步骤9,处理网络服务器计算机120可以将授权响应消息转发到传送计算机115,然后转发到资源提供商计算机110。处理网络服务器计算机120还可以将消息传输到移动网络运营商计算机系统140,通知移动网络运营商计算机系统140刚开展交易。

[0081] 在一些示例中,授权实体计算机130随后可以完成与移动网络运营商计算机系统140的交互。这可包括在清算和结算程序时在移动网络运营商计算机系统140与授权实体计算机130之间转移资金。

[0082] 在步骤10,可进行清算和结算过程。在一天结束时或在任何其它合适的时间段,可以在传送计算机115与授权实体计算机130之间进行结算,或者可以直接与移动网络运营商计算机系统140进行结算。如果授权实体计算机130与传送计算机115结算,授权实体计算机130可以请求来自移动网络运营商计算机系统140的报销(针对任何费用调整)。移动网络运营商计算机系统140随后可以随由移动网络运营商计算机系统140提供的用户的每月电话账单发票一起为用户开具发票。

[0083] 移动网络运营商计算机系统140可以为通信装置102的用户生成发票。发票可以包括在通信装置102与移动网络运营商计算机系统140之间进行的任何交易,以及在任何资源提供商计算机中的通信装置102之间进行的任何交易。发票中列出的交易可以针对资源提供商计算机110汇总,或根据交易和交易进行的时间单独提供。用户可以向移动网络运营商计算机系统140提供费用报销。

[0084] 也可以交换手续费。例如,授权实体计算机130可以向处理网络服务器计算机120

支付手续费。资源提供商计算机110可以至少部分地基于与绑定到虚拟访问凭证的已批准金额相对应的用户账户的授信和建立而向授权实体计算机130支付手续费。授权实体计算机130可以请求来自移动网络运营商计算机系统140的报销。移动网络运营商计算机系统140可以使用电话账单向通信装置102的用户收费。

[0085] 还可以使用图1描述其它实施例。例如,在图1的附加实施例的步骤1,通信装置102可以与资源提供商计算机110交互,以访问由资源提供商计算机管理的资源。通信装置102可以经由交互站点112或通信装置102的显示屏上的应用程序与资源提供商计算机110交互。

[0086] 在步骤2,资源提供商计算机110可以生成虚拟访问凭证请求并将其传输到处理网络服务器计算机120。虚拟访问凭证请求可以标识用户与通信装置102相对应。此信息可以支持对交互授权的请求(例如,获取对受限区域或资源的访问权限等)。

[0087] 在步骤3,处理网络服务器计算机120可以与授权实体计算机130通信以请求访问。授权实体计算机130可以生成虚拟访问凭证。

[0088] 在一些示例中,授权实体计算机130可以充当初始网关,以确定是否应授权访问权限(例如,对资源提供商计算机110的限制信息的访问权限)。授权实体计算机130可以直接与通信装置102相对应(或经由处理网络服务器计算机120与通信装置102相对应),以请求来自通信装置102的初始认证响应,包括用户的密码或其它唯一标识符。通信装置102可以用密码或其它唯一标识符响应授权实体计算机130,此时授权实体计算机130可以生成虚拟访问凭证。

[0089] 在一些示例中,授权实体计算机130可以与移动网络运营商计算机系统140相对应,以访问有关通信装置102的附加信息,包括订单历史记录、位置历史记录或与通信装置102相关联的用户配置文件信息。例如,移动网络运营商计算机系统140可以向通信装置102提供移动网络服务,并使用与通信装置102的位置跟踪相关联的全球定位系统(GPS)存储位置信息的历史记录。在一些情况下,移动网络运营商计算机系统140可以将此信息提供给授权实体计算机130,以发起与通信装置102的第一认证过程。

[0090] 在步骤4,授权实体计算机130可以向处理网络服务器计算机120提供虚拟访问凭证(例如,在从用户接收到密码或其它唯一标识符等时)。

[0091] 在步骤5,处理网络服务器计算机120可以将虚拟访问凭证从授权实体计算机130传输到资源提供商计算机110或通信装置102以进行处理。资源提供商计算机110可以至少部分地基于接收到虚拟访问凭证而发起允许对资源的访问的过程。例如,资源提供商计算机110可以生成包括虚拟访问凭证的授权请求消息。

[0092] 在步骤6,资源提供商计算机110可以将包括虚拟访问凭证的授权请求消息传输到传送计算机115。传送计算机115可以将授权请求消息传输到处理网络服务器计算机120。处理网络服务器计算机120可以接收包括虚拟访问凭证的授权请求消息,其中授权请求消息请求对交互的授权。

[0093] 在步骤7,处理网络服务器计算机120可以将授权请求消息转发到授权实体计算机130。授权实体计算机130可以至少部分地基于将来自初始认证过程的虚拟访问凭证与授权请求消息中包括的用户信息进行比较来确定是允许还是拒绝访问。此比较和匹配可以与第二级认证相对应。

[0094] 在步骤8,授权实体计算机130可以生成包括批准或拒绝对处理网络服务器计算机120的访问的授权响应消息。处理网络服务器计算机120可以从授权实体计算机130接收授权响应消息。

[0095] 在步骤9,处理网络服务器计算机120可以将授权响应消息转发到传送计算机115,然后转发到资源提供商计算机110。

[0096] 在步骤10,在授权实体计算机130、传送计算机115和移动网络运营商计算机系统140之间可能进行附加交互,包括允许访问由资源提供商110提供的资源。

[0097] 应注意,虽然上述示例与支付相关,但应理解实施例不限于此。其它实施例可以涉及可生成虚拟访问凭证以访问来自远程服务器计算机的安全位置或安全数据的系统和方法。

[0098] 贯穿应用程序描述了技术改进。常规系统可以为交互提供单次的认证或授权。本公开的实施例可以包括双认证或授权协议,包括由授权实体计算机执行的第一过程以及由移动网络运营商计算机系统执行的第二过程。此双层认证或授权协议可以提供在用户与资源之间的交互之前的改进的技术确认,从而提供更大的安全性。

[0099] 此外,实施例还允许没有凭证的用户获取临时凭证,使得他们可以访问所需资源,例如数据、位置、商品或服务。实施例可以执行这一操作,而不会对访问基础架构进行重大更改。

[0100] 本文描述的计算机系统可以在硬件中体现,并且包括可适用于实现此类功能的图中的一个或多个元件。可以与计算系统结合的此类系统或部件的示例可以经由系统总线互连。可以提供附加子系统,例如打印机、键盘、固定磁盘或包括计算机可读介质的其它存储器、监视器或其它部件。监视器可以与显示适配器耦合。外围设备和其它输入/输出(I/O)装置可以与I/O控制器耦合,并且可以通过本领域已知的任何数量的构件(例如串行端口)连接到计算机系统。例如,串行端口或其它外部接口可用于将计算机系统连接到例如因特网的广域网、鼠标输入装置或扫描仪。经由系统总线的互连允许中央处理器与每个系统通信,且控制来自系统存储器或固定磁盘的指令的执行以及子系统之间的信息交换。这是可以体现计算机可读介质的存储器和/或固定磁盘。

[0101] 此外,尽管已经使用形式为控制逻辑和编程代码和指令的硬件和软件的特定组合描述了本公开,但应认识到,硬件和软件的其他组合也在本申请的范围内。本申请可以仅以硬件,仅以软件或其组合来实现。

[0102] 本申请中描述的任何软件部件或功能可以使用例如常规的或面向对象的技术并且使用任何合适的计算机语言(例如,Java、C++或Perl)实现为由处理器执行的软件代码。软件代码可以存储为例如随机存取存储器(RAM)、只读存储器(ROM)、例如硬盘驱动器或软盘的磁性介质或例如CD-ROM的光学介质的计算机可读介质上的一系列指令或命令。任何此类计算机可读介质可驻存在单个计算装置上或单个计算装置内,并且可以存在于系统或网络内的不同计算装置上或不同计算装置内。

[0103] 以上描述是说明性的而非限制性的。本发明的许多变化在本领域的技术人员查阅本公开时可变得显而易见。因此,本发明的范围可不参考以上描述来确定,而是可参考待决的权利要求以及其完整范围或等同物来确定。

[0104] 在不脱离本发明的范围的情况下,任何实施例的一个或多个特征可与任何其它实

施例的一个或多个特征组合。

[0105] 除非明确指示有相反的意思,否则“一”或“所述”的叙述旨在表示“一个或多个”。

[0106] 上文提及的所有专利、专利申请、公开案和描述都出于所有目的以全文引用的方式并入。并非承认它们是现有技术。

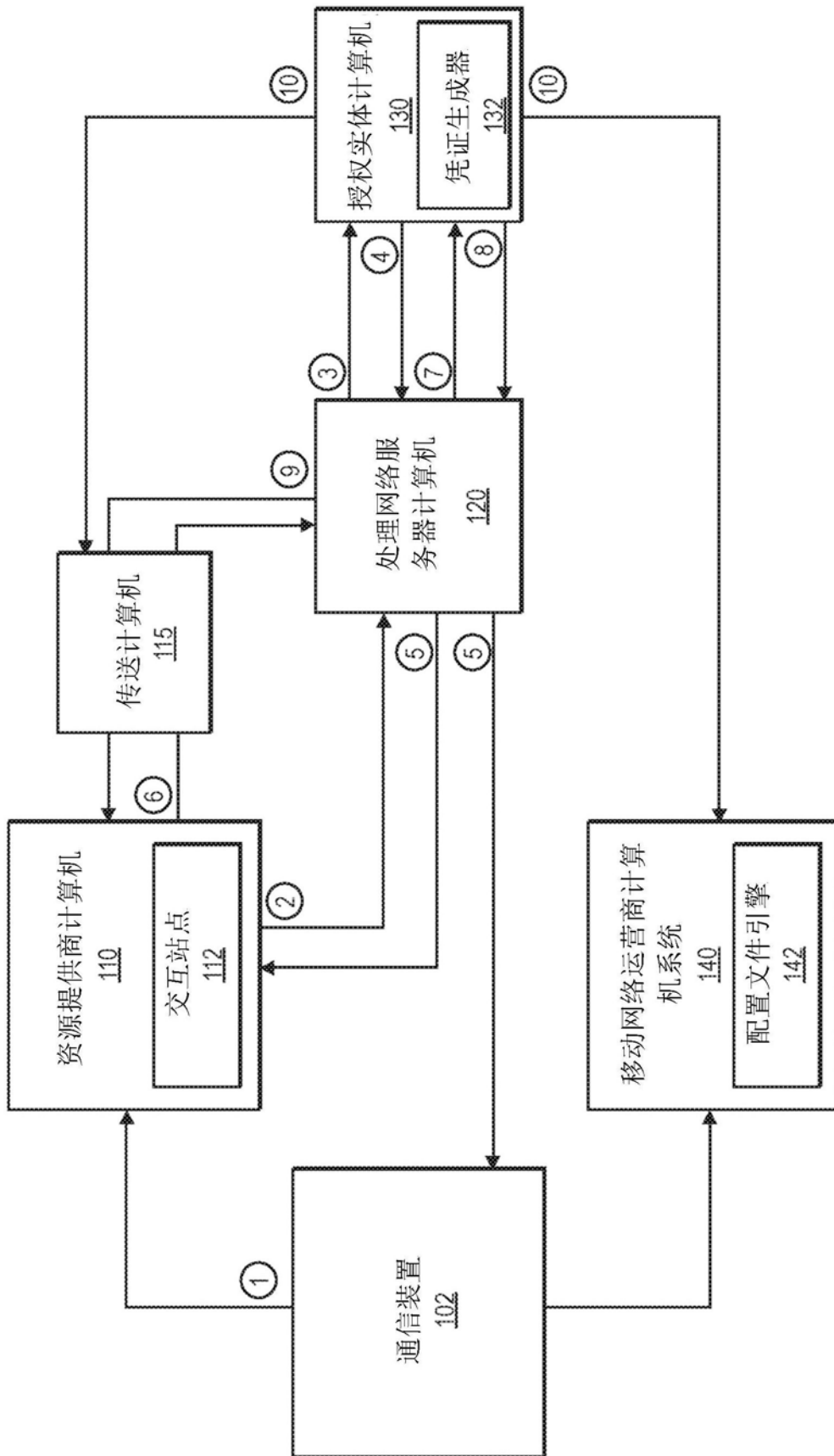


图1

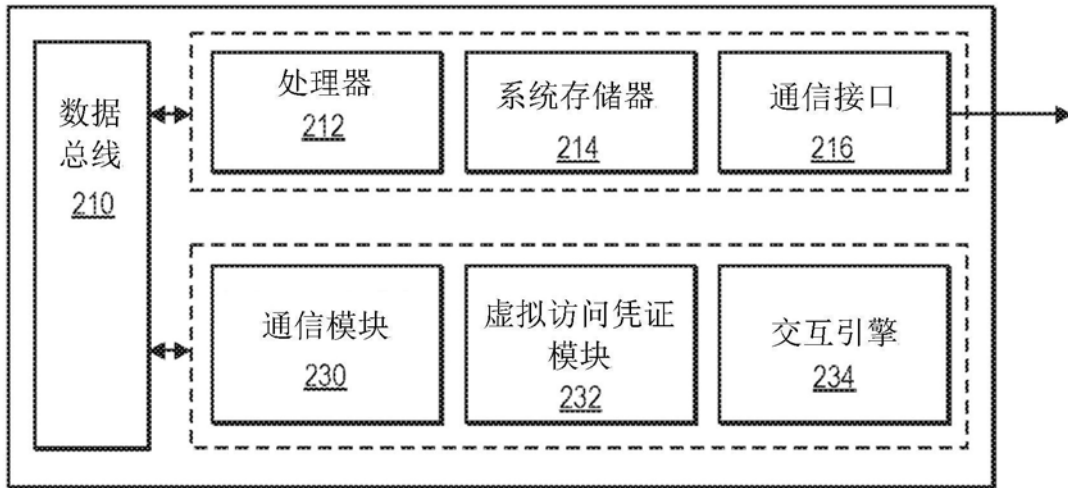


图2

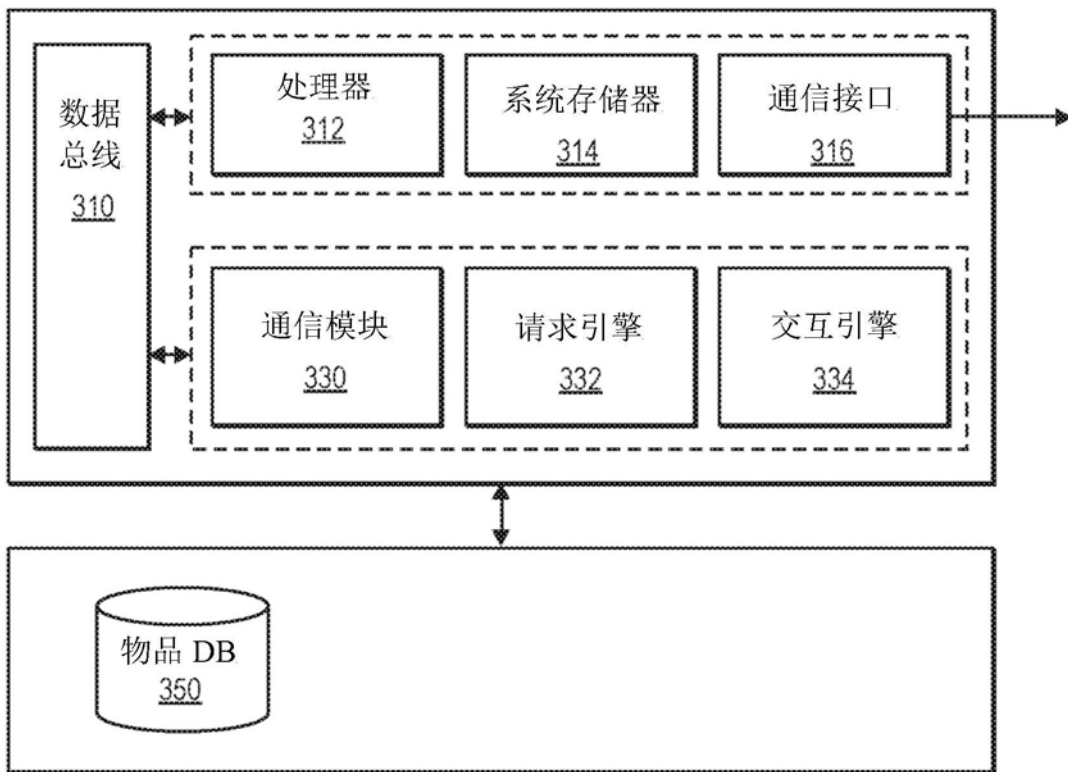


图3

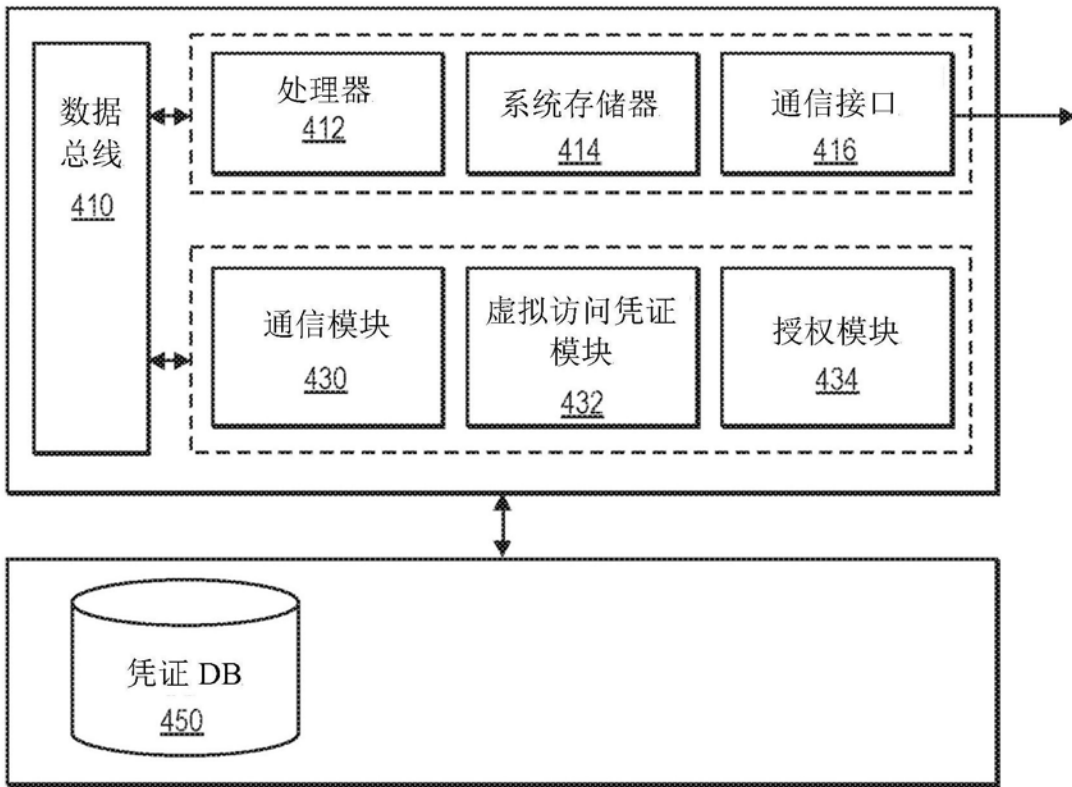


图4

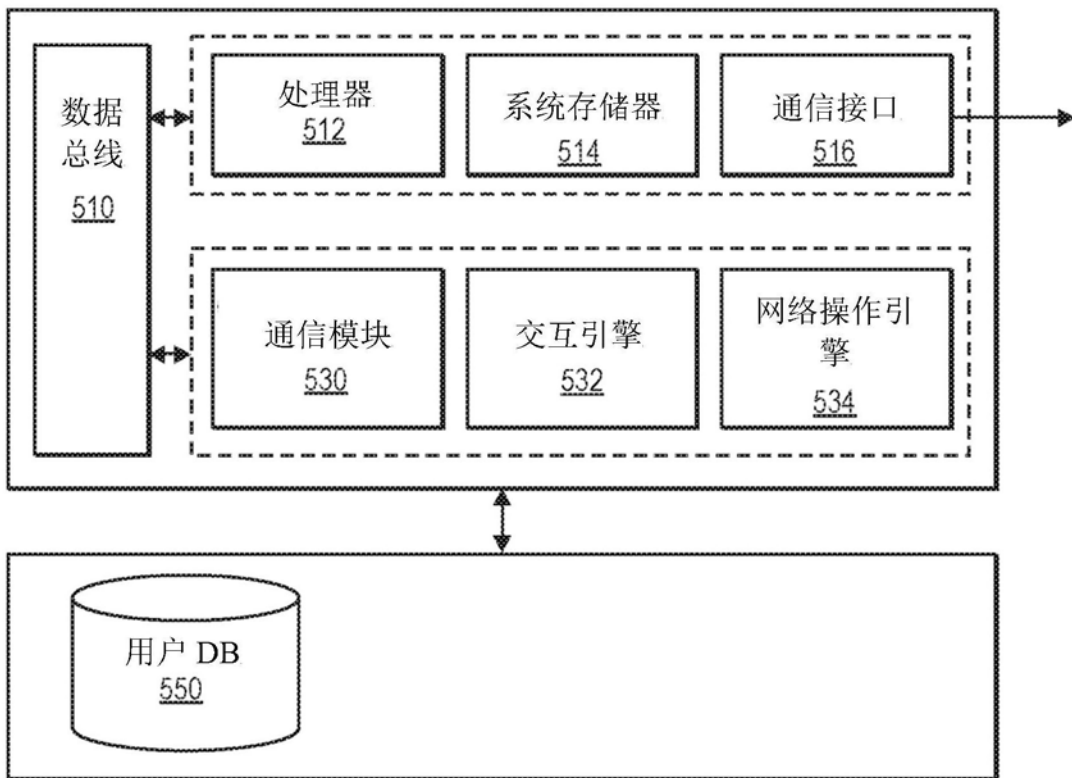


图5

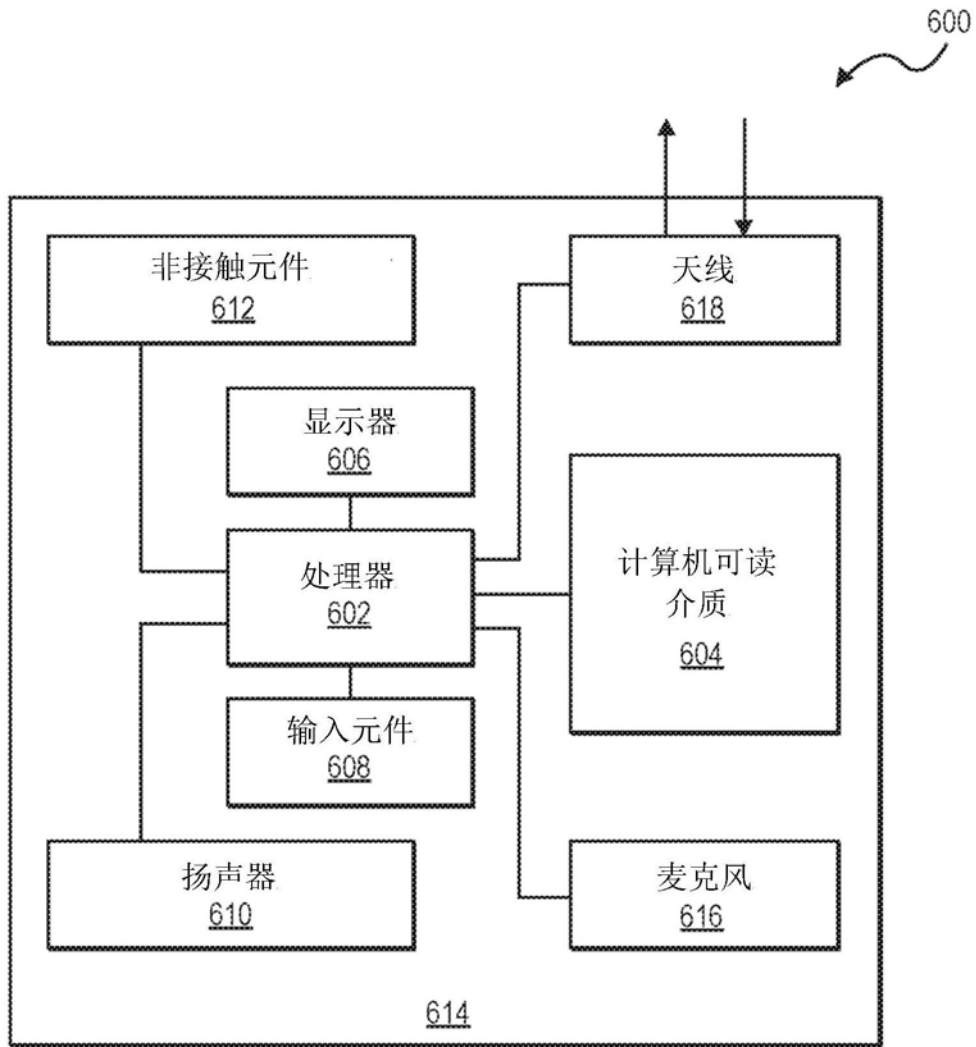


图6